UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/930,029	08/14/2001	William B. Sweet	00131-000100000	3170

31064 7590 10/15/2007

WIESNER & ASSOCIATES
366 CAMBRIDGE AVENUE
PALO ALTO, CA 94301

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
10/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/930,029	SWEET ET AL.	
	Examiner	Art Unit	
	Jeffrey D. Popham	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22 and 52-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22 and 52-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Remarks

Claims 1-22 and 52-58 are pending.

Response to Arguments

1. Applicant's arguments filed 3/6/2007 have been fully considered but they are not persuasive.

Applicant argues that Colosso does not teach receiving a request for an access permission security profile on behalf of a network user. Regarding this argument, Applicant goes on to say that Colosso teaches a customer requesting a key and receiving such key once they have been properly authenticated. Further, Applicant states that the key requested in Colosso does not concern encrypting or decrypting objects to gain access but instead turning on licensed software; and if the customer in Colosso wanted to access the licensed software, they could simply edit the software to view in a binary format or apply a reverse compiler to view the assembly code or source code. The Examiner cannot find where Colosso discloses editing software to view a binary format or applying a reverse compiler to view the assembly or source code. To the contrary, Colosso is concerned with disallowing installation and activation of a product without the appropriate key information (Column 8, line 55 to Column 9, line 6; and Column 12, line 65 to Column 13, line 6, for example). Additionally noted is that an "object" need not be software. An "object" may be any piece of data. As Applicant has described on page 13 of the response, "the customer in Colosso requests a key and receives a key once they have properly authenticated themselves and their purchase of

the licensed software." Here, we can see a request for an access permission security profile. As Applicant further describes on page 17 of the response, "Colosso uses a first cryptographic key (referred to as an installation key) and a customer domain name to decrypt a second cryptographic key (referred to as an activation key)." As Applicant shows here, an object is being decrypted by the requested access permission security profile.

Applicant goes on to argue that there is no mention of both encrypting the licensed software and decrypting the licensed software. As described above, an object is any data, and not necessarily "licensed software".

Applicant also argues that Colosso does not teach securely transmitting the access permission security profile to the network user over the network. Applicant furthers this argument, by referring to claim 2, which describes creating the access permission security profile as identifying one or more groups of users to be provided with cryptographic capabilities, establishing one or more access codes combinable with other components to form a cryptographic key, and creating one or more security profiles for each network user, wherein each security profile contains at least one access code. From claim 2, one can clearly see that Colosso provides an access permission security profile, for example, in the form of an installation key, which is combined with other components (domain name, for example) in order to produce a cryptographic key. The transmission of such an access permission security profile is secured by encrypting the access permission security profile, as shown, for example, in column 15, lines 29-44.

Applicant also argues, regarding claim 2, that Colosso does not teach creating a group of network users with cryptographic capabilities. Since claim 2 recites "identifying one or more groups of network users", the creating of groups is deemed insignificant to the claims. Applicant argues, regarding claim 3, that it also follows that Colosso does not disclose or suggest that each group is a category, organization, organization unit, role, work project, geographical location, workgroup, or domain. As described, by Applicant, on page 17 of the response, Colosso uses a first cryptographic key and a customer domain name in order to decrypt a second key. Since Applicant has shown that a group can be a domain within Colosso, and such domain name is used to decrypt an object, Colosso clearly teaches that a group can be at least a domain.

Applicant also argues that Colosso does not receive from the user information associated with the encrypted object. To the contrary, Colosso describes receiving from the user multiple pieces of information, all of which may be associated with the encrypted object. Some of this information is shown in column 14, lines 31-64, showing information sent from the user, received, and stored in association with the encrypted object. Other arguments regarding Colosso and other claims are equivalent to the arguments above.

Applicant argues that Halter does not teach providing an access permission security profile, but only a unique customer key. As described above, and reiterated here, an "access permission security profile" is not as narrow as Applicant believes. In order to determine the profile's scope, one must view the claimed subject matter. As defined by claim 1, an access permission security profile is "to be used in forming a

cryptographic key". Therefore, for rejection of claim 1, one must only have some piece of data to be used in forming a cryptographic key in order to show an access permission security profile. As further described in claim 2, the creating step comprises creating one or more security profiles for each network user, wherein each security profile contains at least one access code, the access code being combinable with other components to form a key. Therefore, all that is required of the claimed access permission security profile of claim 2 is that it contains an access code that can be used to form a key. As can be seen in the cited section (Column 8, line 61 to Column 10, line 16), one or more keys are encrypted and transmitted. Such encrypted keys are combinable with other components (such as an appropriate decryption key) in order to obtain the keys required to decrypt data (or other keys). Therefore, Halter clearly discloses providing an access permission security profile, as claimed.

Applicant also argues that Halter does not teach a cryptographic key capable of decrypting selected portions of an encrypted object. As described in the cited section (Column 8, line 61 to Column 10, line 16), a user will be provided with keys used to decrypt only the data that the user is allowed to access (such as when the user purchases particular software or multimedia).

Applicant also argues that Halter does not teach securely transmitting the access permission security profile to the network user over the network. In regard to this argument, Applicant argues that Halter teaches away from secure communication suggesting that the keys are delivered to a person orally over a phone. Although Applicant has cited column 9, lines 18-21 to show this telephonic conversation, it

appears as though column 9, lines 13-16 has been overlooked. Column 9, lines 13-16 clearly shows transmitting the access permission security profile (as described above) to the network user over the network, in that "Key distribution means 31 can be a communications channel permitting the key to be electronically transmitted from software distribution processor 10 to user processor 20." As described immediately preceding this section of the current paragraph, the keys are encrypted prior to distribution. The mere fact that Halter provides additional mechanisms for distributing keys is insignificant to the rejection, as such are merely extra functionality within Halter.

Applicant additionally argues that "Clearly, Haller did not disclose, suggest or contemplate any form of secure communication and neither has Win." However, there are many forms of secure communication within both references. A quick glance at the abstract, figures, specification, or claims of either reference will show such. As described above, Halter teaches securely transmitting the access permission security profile to the network user over a network. Halter also teaches securely transmitting encrypted objects. Other portions of Halter describe more about secure communications. Win teaches secure communication of keys, cookies, profiles, objects, and the like, as well as using session and transaction security via SSL.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-6, 15, 16, 19, 20, and 52-57 are rejected under 35 U.S.C. 102(e) as being anticipated by Colosso (U.S. Patent 6,169,976).

Regarding Claim 1,

Colosso discloses a method for providing cryptographic capabilities to a plurality of network users over a decentralized public network comprising receiving a request for an access permission security profile on behalf of a network user (Column 8, line 55 to Column 9, line 39; and Column 13, lines 7-19); authenticating the request (Column 10, lines 25-49; and Column 11, lines 9-34); creating the access permission security profile to be used in forming a cryptographic key for enabling the network user to decrypt selected portions of an encrypted object and to encrypt selected portions of a plaintext object (Column 8, line 55 to Column 9, line 39; and Column 12, line 65 to Column 15, line 25); and securely transmitting the access permission security profile to the network user over the network (Column 12, line 65 to Column 15, line 25).

Regarding Claim 2,

Colosso discloses that the creating step comprises identifying one or more groups of network users who are to be provided with cryptographic capabilities; establishing one or more access codes for each

group wherein each access code is adapted to be combined with other components to form a cryptographic key; and creating one or more security profiles for each network user, wherein each security profile contains at least one access code (Column 12, line 65 to Column 16, line 9).

Regarding Claim 3,

Colosso discloses that each group is a category, organization, organization unit, role, work project, geographical location, workgroup, or domain (Column 11, line 57 to Column 12, line 18).

Regarding Claim 4,

Colosso discloses a method for providing decryption capabilities to a plurality of network users over a decentralized public network comprising receiving a request for decryption capabilities on behalf of a network user (Column 8, line 55 to Column 9, line 39; and Column 13, lines 7-19); authenticating the request (Column 10, lines 25-49; and Column 11, lines 9-34); creating an access permission security profile to be used in forming a cryptographic key for enabling the network user to decrypt an encrypted object (Column 8, line 55 to Column 9, line 39; and Column 12, line 65 to Column 15, line 25); receiving from the user information associated with the encrypted object (Column 12, line 65 to Column 15, line 25); generating a cryptographic key using the access permission security profile and the received information associated with the encrypted object

(Column 12, lien 65 to Column 15, line 25); and securely transmitting the cryptographic key to the network user over the network (Column 12, line 65 to Column 15, line 25).

Regarding Claim 5,

Colosso discloses that the creating step includes identifying one or more groups of network users who are to be provided with cryptographic capabilities; establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key; and creating one or more security profiles for each network user, wherein each security profile contains at least one access code (Column 12, line 65 to Column 16, line 9).

Regarding Claim 6,

Colosso discloses that each group is a category, organization, organization unit, role, work project, geographical location, workgroup, or domain (Column 11, line 57 to Column 12, line 18).

Regarding Claim 52,

Colosso discloses a centralized security management system for distributing cryptographic capabilities to a plurality of network users over a decentralized public network comprising a plurality of member tokens for providing cryptographic capabilities to authenticated users of the decentralized public network (Column 12, line 65 to Column 15, line 25); a

set of server systems for managing the distribution of the member tokens (Column 12, line 65 to Column 15, line 25); means for requesting a member token from at least one server system (Column 8, line 55 to Column 9, line 39; and Column 13, lines 7-19); a set of client systems, wherein each client system includes means for receiving the requested member token and means for utilizing the cryptographic capabilities provided by the member token for selective encryption and decryption (Column 12, line 65 to Column 16, line 56); and means for securely distributing a requested member token from at least one server system to at least one client system over the decentralized public network (Column 12, line 65 to Column 15, line 25).

Regarding Claim 54,

Colosso discloses that the means for requesting a member token resides on each client system (Column 8, line 55 to Column 9, line 39; and Column 13, lines 7-19).

Regarding Claim 55,

Colosso discloses that means for authenticating a user resides on at least one server system (Column 12, line 65 to Column 15, line 25).

Regarding Claim 56,

Colosso discloses that managing the distribution of the member tokens includes dynamic updating of the member tokens (Column 16, line 60 to Column 18, line 2).

Regarding Claim 15,

With respect to claims 1 and 4, Colosso discloses that the request is initiated in band by the network user over the network (Column 8, line 55 to Column 9, line 39; and Column 13, lines 7-19).

Regarding Claim 16,

With respect to claims 1 and 4, Colosso discloses that the access permission security profile is in the form of a token that is adaptable to expire (Column 14, line 65 to Column 15, line 25).

Regarding Claim 19,

With respect to claims 1 and 4, Colosso discloses that the authenticating step includes the use of a software token (Column 10, lines 25-49; and Column 11, lines 9-34).

Regarding Claim 20,

With respect to claims 1 and 4, Colosso discloses that the authenticating step includes the use of a user password (Column 10, lines 25-49; and Column 11, lines 9-34).

Regarding Claim 57,

With respect to claims 1, 4, and 52, Colosso discloses that the decentralized public network is the Internet (Column 6, lines 15-29).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 7-11, 13-16, 19, 20, and 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Colosso in view of Shanton (U.S. Patent 5,680,452).

Regarding Claim 7,

Colosso discloses a method for cryptographically securing the distribution of information over a decentralized public network to a plurality of network users comprising:

Creating a computer representable data object (Column 1, lines 16-21);

Creating one or more access permission credentials (Column 8, line 55 to Column 9, line 39; and Column 12, line 65 to Column 15, line 25);

Assigning an access permission credential wherein the access permission credential ensures that only authorized users are able to decrypt encrypted objects (Column 12, line 65 to Column 15, line 25);

Authorizing at least one network user from the plurality of network users (Column 12, line 65 to Column 15, line 25); and

Transmitting the data object over the network (Column 12, lines 49-57);

But does not disclose the use of embedded objects within an object.

Shanton, however, discloses creating a computer representable data object including one or more embedded objects (Column 9, line 63 to Column 10, line 10); selecting one or more embedded objects of the data to be encrypted (Column 8, lines 1-42; and Column 9, line 63 to Column 10, line 10); encrypting the selected embedded objects (Column 8, lines 1-42; and Column 9, line 63 to Column 10, line 10); and assigning access rights to each of the selected embedded objects, such that only authorized users are able to decrypt encrypted embedded objects of the data object (Column 8, line 1 to Column 9, line 23). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the embedded object protection system of Shanton into the licensing system of Colosso in order to allow the system to be more flexible and offer still more protection, as well as to provide the ability to distribute the same object to many users, while allowing each user to have access to a personalized subset of the embedded objects.

Regarding Claim 8,

Colosso as modified by Shanton discloses the method of claim 7, in addition, Shanton discloses that the information is digital content (Column 4, line 38 to Column 5, line 9).

Regarding Claim 9,

Colosso as modified by Shanton discloses the method of claim 7, in addition, Colosso discloses that the authorizing step includes receiving a request for an access permission security profile on behalf of a network user, authenticating the request, and securely transmitting the security profile to the network user over the network (Column 8, line 55 to Column 9, line 39; and Column 12, line 65 to Column 15, line 25).

Regarding Claim 10,

Colosso as modified by Shanton discloses the method of claim 7, in addition, Colosso discloses that the authorizing step includes sending a request for an access permission security profile on behalf of a network user to a centralized server system over the network, receiving the request at the centralized server system, authenticating the request, and securely transmitting the access permission security profile from the server system to the network user over the network (Column 8, line 55 to Column 9, line 39; and Column 12, line 65 to Column 15, line 25).

Regarding Claim 11,

Colosso as modified by Shanton discloses the method of claim 7, in addition, Colosso discloses that the authorizing step is automatic and based upon the user's possession of an access permission security profile (Column 12, line 65 to Column 15, line 25).

Regarding Claim 12,

Colosso as modified by Shanton discloses the method of claim 7, in addition, Colosso discloses that the encrypting step comprises identifying a group of network users who are to be allowed access to a data object to be encrypted; generating an appropriate cryptographic credential key from a set of credential categories, the credential key relating to the group of network users; generating a cryptographic working key from at least a domain component, a maintenance component, and a pseudorandom component; encrypting the data object with the working key; encrypting the pseudorandom component with the credential key; and associating the encrypted pseudorandom component with the encrypted data object (Column 12, line 65 to Column 15, line 25).

Regarding Claim 13,

Colosso as modified by Shanton discloses the method of claim 10, in addition, Colosso discloses that the access permission security profile is created by identifying one or more groups of network users who are to be provided with cryptographic capabilities; establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key; and creating one or more security profiles for each network user, wherein each security profile contains at least one access code (Column 12, line 65 to Column 16, line 9).

Regarding Claim 14,

Colosso as modified by Shanton discloses the method of claim 13, in addition, Colosso discloses that each group is a category, organization, organization unit, role, work project, geographical location, workgroup, or domain (Column 11, line 57 to Column 12, line 18).

Regarding Claim 15,

Colosso as modified by Shanton discloses the method of claim 9, in addition, Colosso discloses that the request is initiated in band by the network user over the network (Column 8, line 55 to Column 9, line 39; and Column 13, lines 7-19).

Regarding Claim 16,

Colosso as modified by Shanton discloses the method of claims 9-11, in addition, Colosso discloses that the access permission security profile is in the form of a token that is adaptable to expire (Column 14, line 65 to Column 15, line 25).

Regarding Claim 19,

Colosso as modified by Shanton discloses the method of claims 9 and 10, in addition, Colosso discloses that the authenticating step includes the use of a software token (Column 10, lines 25-49; and Column 11, lines 9-34).

Regarding Claim 20,

Colosso as modified by Shanton discloses the method of claims 9 and 10, in addition, Colosso discloses that the authenticating step includes

the use of a user password (Column 10, lines 25-49; and Column 11, lines 9-34).

Regarding Claim 53,

Colosso does not explicitly disclose that each client system further includes user authentication means.

Shanton, however, discloses that each client system further includes user authentication means (Column 8, lines 1-42). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the embedded object protection system of Shanton into the licensing system of Colosso in order to allow the system to be more flexible and offer still more protection, as well as to provide the ability to distribute the same object to many users, while allowing each user to have access to a personalized subset of the embedded objects.

Regarding Claim 57,

Colosso as modified by Shanton discloses the method of claim 7, in addition, Colosso discloses that the decentralized public network is the Internet (Column 6, lines 15-29).

4. Claims 17, 18, and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Colosso in view of Kennedy (U.S. Patent 6,084,968).

Regarding Claim 17,

Colosso discloses the methods of claims 1 and 4, but does not disclose that the authenticating step includes the use of biometric information.

Kennedy, however, discloses that the authenticating step includes the use of biometric information (Column 3, line 8 to Column 4, line 38). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the security token of Kennedy into the licensing system of Colosso in order to provide for secure authentication of a user via biometrics, which are much more difficult to forge or break than a simple user password.

Regarding Claim 18,

Colosso discloses the methods of claims 1 and 4, but does not disclose that the authenticating step includes the use of a hardware token.

Kennedy, however, discloses that the authenticating step includes the use of a hardware token (Column 3, line 8 to Column 4, line 38). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the security token of Kennedy into the licensing system of Colosso in order to provide for secure authentication of a user via biometrics, which are much more difficult to forge or break than a simple user password.

Regarding Claim 58,

Colosso discloses the methods of claims 1 and 4, but does not disclose that the decentralized public network is a cellular phone network.

Kennedy, however, discloses that the decentralized public network is a cellular phone network (Column 3, line 8 to Column 4, line 38). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the security token of Kennedy into the licensing system of Colosso in order to provide for secure authentication of a user via biometrics, which are much more difficult to forge or break than a simple user password.

5. Claims 17, 18, and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Colosso in view of Shanton, further in view of Kennedy.

Regarding Claim 17,

Colosso as modified by Shanton discloses the methods of claims 9 and 10, but does not disclose that the authenticating step includes the use of biometric information.

Kennedy, however, discloses that the authenticating step includes the use of biometric information (Column 3, line 8 to Column 4, line 38). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the security token of Kennedy into the licensing system of Colosso as modified by Shanton in order to provide for

secure authentication of a user via biometrics, which are much more difficult to forge or break than a simple user password.

Regarding Claim 18,

Colosso as modified by Shanton discloses the methods of claims 9 and 10, but does not disclose that the authenticating step includes the use of a hardware token.

Kennedy, however, discloses that the authenticating step includes the use of a hardware token (Column 3, line 8 to Column 4, line 38). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the security token of Kennedy into the licensing system of Colosso as modified by Shanton in order to provide for secure authentication of a user via biometrics, which are much more difficult to forge or break than a simple user password.

Regarding Claim 58,

Colosso as modified by Shanton discloses the methods of claims 9 and 10, but does not disclose that the decentralized public network is a cellular phone network.

Kennedy, however, discloses that the decentralized public network is a cellular phone network (Column 3, line 8 to Column 4, line 38). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the security token of Kennedy into the licensing system of Colosso as modified by Shanton in order to provide for

secure authentication of a user via biometrics, which are much more difficult to forge or break than a simple user password.

6. Claims 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Colosso in view of Win.

Regarding Claim 21,

Colosso does not disclose that the authenticating step includes the use of a record of time at which the request was made.

Win, however, discloses that the authenticating step includes the use of a record of time at which the request was made (Column 9, lines 46-52; and Column 15, lines 46-60). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the role-based access control system of Win into the licensing system of Colosso in order to detect login anomalies and take action against such anomalies in order to further protect against unauthorized access.

Regarding Claim 22,

Colosso does not disclose that the authenticating step includes the use of a record of the user's physical location.

Win, however, discloses that the authenticating step includes the use of a record of the user's physical location (Column 9, lines 46-52; and Column 15, lines 46-60). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the role-

based access control system of Win into the licensing system of Colosso in order to detect login anomalies and take action against such anomalies in order to further protect against unauthorized access.

7. Claims 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Colosso in view of Shanton, further in view of Win.

Regarding Claim 21,

Colosso as modified by Shanton does not disclose that the authenticating step includes the use of a record of time at which the request was made.

Win, however, discloses that the authenticating step includes the use of a record of time at which the request was made (Column 9, lines 46-52; and Column 15, lines 46-60). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the role-based access control system of Win into the licensing system of Colosso as modified by Shanton in order to detect login anomalies and take action against such anomalies in order to further protect against unauthorized access.

Regarding Claim 22,

Colosso as modified by Shanton does not disclose that the authenticating step includes the use of a record of the user's physical location.

Win, however, discloses that the authenticating step includes the use of a record of the user's physical location (Column 9, lines 46-52; and Column 15, lines 46-60). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the role-based access control system of Win into the licensing system of Colosso as modified by Shanton in order to detect login anomalies and take action against such anomalies in order to further protect against unauthorized access.

8. Claims 1-16, 18-22, 52, and 54-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Halter (U.S. Patent 5,319,705) in view of Win (U.S. Patent 6,161,139).

Regarding Claim 1,

Halter discloses a method for providing cryptographic capabilities to a plurality of network users over a decentralized public network comprising receiving a request for an access permission security profile on behalf of a network user (Column 8, line 61 to Column 9, line 27); creating the access permission security profile to be used in forming a cryptographic key for enabling the network user to decrypt selected portions of an encrypted object and to encrypt selected portions of a plaintext object (Column 8, line 61 to Column 10, line 16); and securely transmitting the access

permission security profile to the network user over the network (Column 8, line 61 to Column 10, line 16);

But does not explicitly disclose authenticating the request.

Win, however, discloses authenticating the request (Column 9, lines 36-45; and Column 10, lines 26-40). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the RBAC system of Win into the access control system of Halter in order to authenticate and authorize a user to access encrypted materials based on roles that are easy to configure, reconfigure, and administer.

Regarding Claim 2,

Halter as modified by Win discloses the method of claim 1, in addition, Halter discloses that the creating step comprises identifying one or more users who are to be provided with cryptographic capabilities; establishing one or more access codes for each user wherein each access code is adapted to be combined with other components to form a cryptographic key; and creating one or more security profiles for each network user, wherein each security profile contains at least one access code (Column 8, line 61 to Column 10, line 16); and Win discloses that the access codes are based upon groups of users (Column 10, lines 26-49; and Column 13, lines 32-44).

Regarding Claim 3,

Halter as modified by Win discloses the method of claim 2, in addition, Win discloses that each group is a category, organization, organization unit, role, work project, geographical location, workgroup, or domain (Column 13, lines 32-44).

Regarding Claim 4,

Halter discloses a method for providing decryption capabilities to a plurality of network users over a decentralized public network comprising receiving a request for decryption capabilities on behalf of a network user (Column 8, line 61 to Column 9, line 27); creating an access permission security profile to be used in forming a cryptographic key for enabling the network user to decrypt an encrypted object (Column 8, line 61 to Column 10, line 16); receiving from the user information associated with the encrypted object (Column 8, line 61 to Column 10, line 16); generating a cryptographic key using the access permission security profile and the received information associated with the encrypted object (Column 8, line 61 to Column 10, line 16); and securely transmitting the cryptographic key to the network user over the network (Column 8, line 61 to Column 10, line 16);

But does not explicitly disclose authenticating the request.

Win, however, discloses authenticating the request (Column 9, lines 36-45; and Column 10, lines 26-40). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to

incorporate the RBAC system of Win into the access control system of Halter in order to authenticate and authorize a user to access encrypted materials based on roles that are easy to configure, reconfigure, and administer.

Regarding Claim 5,

Halter as modified by Win discloses the method of claim 4, in addition, Halter discloses that the creating step comprises identifying one or more users who are to be provided with cryptographic capabilities; establishing one or more access codes for each user wherein each access code is adapted to be combined with other components to form a cryptographic key; and creating one or more security profiles for each network user, wherein each security profile contains at least one access code (Column 8, line 61 to Column 10, line 16); and Win discloses that the access codes are based upon groups of users (Column 10, lines 26-49; and Column 13, lines 32-44).

Regarding Claim 6,

Halter as modified by Win discloses the method of claim 5, in addition, Win discloses that each group is a category, organization, organization unit, role, work project, geographical location, workgroup, or domain (Column 13, lines 32-44).

Regarding Claim 7,

Halter discloses a method for cryptographically securing the distribution of information over a decentralized public network to a plurality of network users comprising:

Creating a computer representable data object including one or more embedded objects (Column 8, line 61 to Column 10, line 16; and Column 23, line 51 to Column 24, line 32);

Selecting one or more embedded objects of the data to be encrypted (Column 8, line 61 to Column 10, line 16; and Column 23, line 51 to Column 24, line 32);

Encrypting the selected embedded objects (Column 8, line 61 to Column 10, line 16; and Column 23, line 51 to Column 24, line 32);

Creating one or more access permission credentials (Column 8, line 61 to Column 10, line 16; and Column 23, line 51 to Column 24, line 32);

Assigning an access permission credential to each of the selected embedded objects, wherein the access permission credential ensures that only authorized users are able to decrypt encrypted embedded objects of the data object (Column 8, line 61 to Column 10, line 16; and Column 23, line 51 to Column 24, line 32);

Transmitting the data object over the network (Column 8, line 61 to Column 10, line 16; and Column 23, line 51 to Column 24, line 32);

But does not explicitly disclose authorizing at least one network user from the plurality of network users.

Win, however, discloses authorizing at least one network user from the plurality of network users (Column 9, lines 36-45; and Column 10, lines 26-40). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the RBAC system of Win into the access control system of Halter in order to authenticate and authorize a user to access encrypted materials based on roles that are easy to configure, reconfigure, and administer.

Regarding Claim 8,

Halter as modified by Win discloses the method of claim 7, in addition, Halter discloses that the information is digital content (Column 7, line 63 to Column 8, line 25).

Regarding Claim 9,

Halter discloses that the authorizing step includes receiving a request for an access permission security profile on behalf of a network user, and securely transmitting the security profile to the network user over the network (Column 8, line 61 to Column 10, line 16); and Win discloses authenticating the request (Column 9, lines 36-45; and Column 10, lines 26-40).

Regarding Claim 10,

Halter discloses that the authorizing step includes sending a request for an access permission security profile on behalf of a network user to a centralized server system over the network, receiving the request at the centralized server system, and securely transmitting the access permission security profile from the server system to the network user over the network (Column 8, line 61 to Column 10, line 16); and Win discloses authenticating the request (Column 9, lines 36-45; and Column 10, lines 26-40).

Regarding Claim 11,

Win discloses that the authorizing step is automatic and based upon the user's possession of an access permission security profile (Column 10, lines 26-40).

Regarding Claim 12,

Halter discloses that the encrypting step comprises identifying an entity who is to be allowed access to a data object to be encrypted; generating an appropriate cryptographic credential key from a set of credential categories, the credential key relating to the entity; generating a cryptographic working key from at least a domain component, a maintenance component, and a pseudorandom component; encrypting the data object with the working key; encrypting the pseudorandom component with the credential key; and associating the encrypted pseudorandom component with the encrypted data object (Column 8, line

61 to Column 10, line 16; and Column 21, line 7 to Column 24, line 32); and win discloses that the entity comprises a group of network users (Column 10, lines 26-49; and Column 13, lines 32-44).

Regarding Claim 13,

Halter discloses that the creating step comprises identifying one or more users who are to be provided with cryptographic capabilities; establishing one or more access codes for each user wherein each access code is adapted to be combined with other components to form a cryptographic key; and creating one or more security profiles for each network user, wherein each security profile contains at least one access code (Column 8, line 61 to Column 10, line 16); and Win discloses that the access codes are based upon groups of users (Column 10, lines 26-49; and Column 13, lines 32-44).

Regarding Claim 14,

Win discloses that each group is a category, organization, organization unit, role, work project, geographical location, workgroup, or domain (Column 13, lines 32-44).

Regarding Claim 15,

Halter as modified by Win discloses claims 1, 4, and 9, in addition, Halter discloses that the request is initiated in band by the network user over the network (Column 8, line 61 to Column 10, line 16).

Regarding Claim 16,

Halter as modified by Win discloses claims 1, 4, 9, 10, and 11, in addition, Win discloses that the access permission security profile is in the form of a token that is adaptable to expire (Column 10, lines 50-62).

Regarding Claim 18,

Halter as modified by Win discloses claims 1, 4, 9, and 10, in addition, Win discloses that the authenticating step includes the use of a hardware token (Column 27, lines 27-40).

Regarding Claim 19,

Halter as modified by Win discloses claims 1, 4, 9, and 10, in addition, Win discloses that the authenticating step includes the use of a software token (Column 17, lines 24-33).

Regarding Claim 20,

Halter as modified by Win discloses claims 1, 4, 9, and 10, in addition, Win discloses that the authenticating step includes the use of a user password (Column 9, lines 25-35).

Regarding Claim 21,

Halter as modified by Win discloses claims 1, 4, 9, and 10, in addition, Win discloses that the authenticating step includes the use of a record of time at which the request was made (Column 9, lines 46-52).

Regarding Claim 22,

Halter as modified by Win discloses claims 1, 4, 9, and 10, in addition, Win discloses that the authenticating step includes the use of a record of the user's physical location (Column 15, lines 46-60).

Regarding Claim 52,

Halter discloses a centralized security management system for distributing cryptographic capabilities to a plurality of network users over a decentralized public network comprising: a plurality of member tokens for providing cryptographic capabilities to users of the decentralized public network (Column 8, line 61 to Column 10, line 16); a set of server systems for managing the distribution of the member tokens (Column 8, line 61 to Column 10, line 16); means for requesting a member token from at least one server system (Column 8, line 61 to Column 10, line 16); a set of client systems, wherein each client system includes means for receiving the requested member token and means for utilizing the cryptographic capabilities provided by the member token for selective encryption and decryption (Column 8, line 61 to Column 10, line 16); and means for securely distributing a requested member token from at least one server system to at least one client system over the decentralized public network (Column 8, line 61 to Column 10, line 16);

But does not explicitly disclose authenticating the request.

Win, however, discloses authenticating the request (Column 9, lines 36-45; and Column 10, lines 26-40). It would have been obvious to

one of ordinary skill in the art at the time of applicant's invention to incorporate the RBAC system of Win into the access control system of Halter in order to authenticate and authorize a user to access encrypted materials based on roles that are easy to configure, reconfigure, and administer.

Regarding Claim 54,

Halter as modified by Win discloses the system of claim 52, in addition, Halter discloses that the means for requesting a member token resides on each client system (Column 8, line 61 to Column 10, line 16).

Regarding Claim 55,

Halter as modified by Win discloses the system of claim 52, in addition, Win discloses that means for authenticating a user resides on at least one server system (Column 10, lines 26-40).

Regarding Claim 56,

Halter as modified by Win discloses the system of claim 52, in addition, Win discloses that managing the distribution of the member tokens includes dynamic updating of the member tokens (Column 17, lines 37-48).

Regarding Claim 57,

Halter as modified by Win discloses claims 1, 4, 7, and 52, in addition, Win discloses that the decentralized public network is the Internet (Column 4, lines 46-57).

9. Claims 17, 53, and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Halter in view of Win, further in view of Kennedy.

Regarding Claim 17,

Halter as modified by Win does not disclose that the authenticating step includes the use of biometric information.

Kennedy, however, discloses that the authenticating step includes the use of biometric information (Column 3, line 8 to Column 4, line 38). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the security token system of Kennedy into the access control system of Halter as modified by Win in order to provide for secure authentication of a user via biometrics, which are much more difficult to forge or break than a simple user password.

Regarding Claim 53,

Halter as modified by Win does not disclose that each client system further includes user authentication means.

Kennedy, however, discloses that each client system further includes user authentication means (Column 3, line 8 to Column 4, line 38). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the security token system of Kennedy into the access control system of Halter as modified by Win in

order to provide for secure authentication of a user via biometrics, which are much more difficult to forge or break than a simple user password.

Regarding Claim 58,

Halter as modified by Win does not disclose that the decentralized public network is a cellular phone network.

Kennedy, however, discloses that the decentralized public network is a cellular phone network (Column 3, line 8 to Column 4, line 38). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the security token system of Kennedy into the access control system of Halter as modified by Win in order to provide for secure authentication of a user via biometrics, which are much more difficult to forge or break than a simple user password.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2137

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER